UNIVERSITY of LUSAKA

Passion for Quality Education: Our Driving Force

SCHOOL OF LAW

THE ADEQUACY AND APPROPRIATENESS OF THE LEGAL FRAMEWORK GOVERNING INTERNET OF THINGS AND INTERNET OF BEINGS IN ZAMBIA

BY

ABIGAIL M.N MWAPULE

LLB22114289

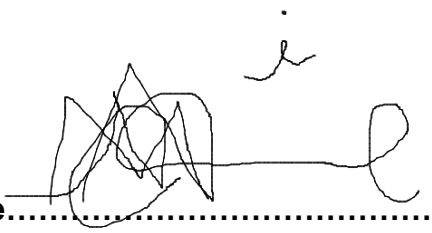
An obligatory essay submitted to the University of Lusaka in partial fulfillment of the requirement for the award of the Bachelor of Laws (LLB) Degree

2025

DECLARATION

I, **ABIGAIL M.N MWAPULE ,** do declare that this dissertation titled **"THE ADEQUACY AND APPROPRIATENESS OF THE LEGAL FRAMEWORK GOVERNING INTERNET OF THINGS AND INTERNET OF BEINGS IN ZAMBIA"** which is hereby submitted to the School of Law at the University of Lusaka as part of the requirements for the award of the Bachelor of Laws (LLB) degree, is my original work and has not previously been submitted for the award of a degree at this or any other tertiary institution.

The sources that have been used or quoted have been indicated and duly acknowledged as complete reference

Signature  **……..**

Date: 14/11/2025

SUPERVISOR'S RECOMMENDATION

I Do hereby recommend that this dissertation titled **"THE ADEQUACY AND APPROPRIATENESS OF THE LEGAL FRAMEWORK GOVERNING INTERNET OF THINGS AND INTERNET OF BEINGS IN ZAMBIA"** done under my supervision, be admitted by the university, I have checked it carefully and I am satisfied that it meets necessary requirements pertaining to the format laid down by the university regulations.

.....

MRS KAPUTO

(Supervisor)

14/ 11/ 2025

(Date)

DEDICATION

This paper is dedicated to my late father, Captain Daniel Kindo Mwapule, whose love of books, critical thinking, and the legal profession inspired my academic and professional path. I gratefully honor his legacy with this work.

I also dedicate this paper to my second father, Vincent Chilenga Nkomeshya, whose unwavering support, guidance, and sponsorship have been vital to my academic journey. I am truly grateful for his generosity and encouragement.

Lastly, I dedicate this paper to my children, Fortune Mathews, Mandisa Abigail, and Mapalo Mandlenkosi Tembo. Your resilience, support, and understanding throughout this course have been invaluable, and I am deeply grateful for your encouragement during all our challenges in this period.

ACKNOWLEDGEMENTS

What a journey, what a story to tell, and what a cloud of witnesses who have carried and supported me through it all, prominent of whom are the following hereby acknowledged:

Firstly, I acknowledge The Only Wise God, the one true God and father of our Lord Jesus Christ, who has been all sufficient, faithful and deeply gracious to me, to whom I owe all that I am and am becoming.

Secondly, I acknowledge and thank my supervisor Mrs. Kaputo for believing in me, believing in my abilities, encouraging me and diligently guiding me through this research process.

I also thank my special friends Mundia, Victoria, Betty and Shadreck and their spouses for supporting this journey in amazingly diverse ways and being such pillars of strength to me.

Many thanks also go to My spiritual mentors – Apostle Michael Orokpo for acting as the last push to my embarking on this journey and the Venerable Canon Father Robert Sihubwa for being a source of guidance and stability as I navigated this journey amidst a very challenging personal situation.

Thank you to Abigail Mwapule Global Foundation team for making this journey easier for me by your dynamism, sacrifice and thoughtfulness.

Lastly, I would like to thank the University of Lusaka for the opportunity to grow by pursuing this degree, for the diverse knowledge and skills imparted and the support given throughout this journey. I am deeply grateful.

TABLE OF CONTENTS

TABLE OF STATUTES

LIST OF CASES

Thomas Mumba v The People (1984) ZR, 38

R (Bridges) v Chief Constable of South Wales Police [2020] EWCA Civ 1058 (Court of Appeal, United Kingdom).

Coalition for Reform and Democracy (CORD) v Attorney General & Another [2015] eKLR. Kenya Law Reports. Available at: https://kenyalaw.org/caselaw/cases/view/108412

ABSTRACT

This study examines the adequacy and appropriateness of Zambia's legal framework governing the Internet of Things (IoT) and the Internet of Beings (IoB). These emerging technologies connect devices and even living beings, creating new opportunities for innovation but also serious legal and ethical challenges. While Zambia has enacted the *Data Protection Act of 2021* and the *Cyber Security Act*, these laws do not adequately address the unique risks that IoT and IoB present, such as violations of privacy, dignity, and bodily autonomy. The research finds that Zambia's current legal framework protects traditional rights but lacks clear rules on the collection, use, and sharing of sensitive biological and neurological data.

Through a comparative analysis, the study draws lessons from the United Kingdom and Kenya, both of which have developed stronger systems for regulating data protection and digital technologies. The UK's *Product Security and Telecommunications Infrastructure Act 2022* and Kenya's *Data Protection Act 2019* demonstrate how privacy-by-design and active enforcement can safeguard citizens in the digital age.

The findings reveal that Zambia needs to strengthen its laws to include explicit protection for biological and mental data, define key terms like "personal use" and "legitimate interest," and empower enforcement agencies. The study concludes that without these reforms, IoT and IoB technologies could threaten constitutional rights such as privacy, dignity, and freedom of thought. It recommends legal amendments, stronger oversight institutions, and clear penalties to ensure technology serves people without undermining their rights.

CHAPTER ONE

1.0 INTRODUCTION

Technology is changing our world faster than ever before. Among the newest changes are the Internet of Things (IoT) and Internet of Beings (IoB), which are changing how we live, work, and connect with each other. IoT connects everyday items like fridges, TVs, and home security systems to the internet, while IoB goes further by connecting living things - including humans - through devices worn on or placed inside the body.[1]

The Internet of Things (IoT) and the Internet of Beings (IoB) are called disruptive technologies because they change the way people, businesses, and governments normally operate. They introduce new ways of connecting devices, people, and data, which can both create opportunities and cause challenges. Because of this, every jurisdiction in the world needs to carefully consider how these technologies will affect its legal system, governance, business practices, daily life of individuals, and the protection of rights under the Constitution.

Internet of Bodies or Internet of Beings involves the use of interconnected devices embedded in human beings (e.g., wearables, implants or sensors relying on proximity) to collect and transmit data about physical, emotional, and behavioural states. The concept of the "Internet of Beings" is an emerging idea that builds on the “Internet of Things” which connects everyday devices to the internet. The concept of Internet of Beings extends the concept of Internet of Things by potentially integrating all living organisms; humans, animals, plants, and even microbes into a connected digital ecosystem. This could involve the use of sensors, biometrics, and artificial intelligence to monitor, track, and interact with the behaviours and states of living beings.

While these technologies offer significant benefits, they also raise critical questions about privacy, autonomy, and the potential for misuse. In Zambia, the legal framework addressing these concerns is still developing. The **Data Protection Act**[2], which came into effect in April 2021, marks a significant step toward regulating the collection and use

[1] __ __https://www.emnify.com/blog/iot-security#:~:text=The%202016%20Mirai%20botnet,but%20also%20because%20the (Accessed 19/04/2025)
[2] Act No. 3 of 2021

of personal data. However, its enforcement began only in March 2025, and it does not specifically address the complexities introduced by IoT and IoB technologies.[3]

This dissertation aims to critically examine the adequacy and appropriateness of Zambia's legal and regulatory framework concerning IoT and IoB. By examining the intersection of these technologies with human rights, the study seeks to identify potential gaps and propose recommendations for a more comprehensive legislative response.

1.1 BACKGROUND OF THE STUDY

The rapid advancement of IoT technologies in Zambia is evident across various sectors. Between them, the technologies can be used to control the actions of human beings. Top on the minds of governments around the world may be the possibility of exploiting Internet of Things to facilitate the confinement of criminals as well as monitor convicts and ex convicts. The possibility of tapping into minds of criminals and ex-convicts and using the technology in combatting criminal activities in other ways may be too tempting a possibility to not take advantage of by some jurisdictions.

For instance, in Lusaka, a water quality monitoring system based on IoT has been developed to detect contamination in real-time, thereby preventing waterborne diseases.[4] Additionally, the agriculture sector is witnessing the adoption of smart farming solutions, with the IoT market projected to reach $240.8 million by 2024 and grow at an annual rate of 12.23% through 2029.[5]

Despite being a major step forward, the legal framework for the Internet of Things (IoT) and the Internet of Beings (IoB) in Zambia is too limited. The Data Protection Act, which only began enforcement in March 2025, doesn't cover essential areas there are no clear rules tailored for smart devices, and vital bodies like the Data Protection Commissioner's office still lack full authority or clarity in implementation.[6] It misses key protections against overbroad inspection, surveillance, and arrest powers that threaten privacy and freedom.[7]

---

[3] ZAMBIA - Enforcement of the Data Protection Act No. 3 of 2021 Begins in March 2025 https://www.nadpa-rapdp.org/en/node/220 (Accessed 19/04/2025)

[4] Soka Zimba, and Christopher Chembe (2022) Model for Water Quality Monitoring Based on Internet of Things Volume6 (Issue1) (2022) Pages44-51

[5] https://www.statista.com/outlook/tmo/internet-of-things/zambia (Accessed 19/04/2025)

[6] https://www.nadpa-rapdp.org/en/node/220?utm (Accessed on 24/08/2025)

[7] https://freedomhouse.org/country/zambia/freedom-net/2022 (Accessed on 24/08/2025)

Plus, with no clear guidance on how to store or transfer data, it's hard for businesses and regulators to navigate cross-border or industrial data, the things IoT and IoB devices generate and share.[8]

The Data Protection Act of 2021, which aims to safeguard personal data, includes broad exceptions for criminal investigations and national security purposes. In addition, the integration of IoT and IoB technologies has prompted discussions about privacy and human rights. In Zambia, the absence of clear legal guidelines raises concerns about the potential infringement of human rights, such as the right to privacy under **Article 17** and the freedom of conscience, belief, and religion under **Article 19 of the Constitution of Zambia**,[9] which are at risk if there is no strong legal framework to guide the use of IoT and IoB. Without proper safeguards, these technologies can easily be misused, leading to unauthorized surveillance, loss of personal privacy, or even control over people's choices, actions, and thoughts.[10]

Furthermore, the **Cyber Security Act**[11], grants law enforcement agencies extensive powers to intercept communications and conduct surveillance with limited oversight. This lack of judicial review and the potential for misuse could lead to the suppression of civil liberties and the erosion of public trust in digital technologies.

The reasons for drawing lessons from the United Kingdom and Kenya, is that with the United Kingdom has pioneered robust legal measures to regulate IoT security, notably through the Product Security and Telecommunications Infrastructure Act 2022 which came into force in April 2024 alongside detailed regulations mandating baseline cybersecurity standards for connectable devices.[12] These frameworks prohibit default passwords, require transparent vulnerability reporting mechanisms, and oblige manufacturers to declare the minimum duration for security updates, enforced through

[8] ZAMBIA - Enforcement of the Data Protection Act No. 3 of 2021 Begins in March 2025 https://www.nadpa-rapdp.org/en/node/220 (Accessed 19/04/2025)
[9] Chapter 1 of the laws of Zambia
[10] https://www.emnify.com/blog/iot-security#:~:text=The%202016%20Mirai%20botnet,but%20also%20because%20the (Accessed 19/04/2025)
[11] Act No. 3 of 2025
[12] Government of the United Kingdom (2024) *Regulations: Consumer connectable product security*. Available at: https://www.gov.uk/guidance/regulations-consumer-connectable-product-security (Accessed: 3 September 2025).

sanctions like fines up to £10 million or 4% of global revenue. Additionally, the UK's Code of Practice for Consumer IoT Security and its integration into legislation exemplify a model of "secure-by-design" regulation.[13] This demonstrates how a developed legal system can proactively safeguard privacy and security in IoT ecosystems.

In contrast, **Kenya's legal landscape** while not explicitly addressing IoT offers adaptable and relevant building blocks. The **Constitution of Kenya (2010)** affirms the right to privacy, and the **Data Protection Act** mandates privacy-by-design and technical safeguards in data processing. Complementing this, the Computer Misuse and Cybercrimes Act (2018) and related criminal procedure laws create a comprehensive framework against digital abuse and cyber threats. Moreover, the Communications Authority of Kenya plays a central role in cybersecurity oversight and ICT regulation. This context provides a solid foundation for Kenya to evolve tailored IoT/IoB provisions responsive to data protection and cybersecurity concerns.[14]

By studying the **UK's explicit and enforceable regulatory measures** alongside **Kenya's foundational principles and institutions**, you can craft practical, context-sensitive recommendations for strengthening Zambia's laws in response to the unique legal and human rights challenges posed by IoT and IoB technologies.

Therefore, this study is crucial in assessing Zambia's preparedness to address the legal and ethical implications of IoT and IoB technologies. By identifying existing gaps and proposing necessary reforms, the research aims to contribute to the development of a legal framework that safeguards individual rights while fostering technological innovation.

1.2 STATEMENT OF THE PROBLEM

Internet of Things and Internet of Beings have the potential of transforming how we live and understand life on earth as well as how business and national governance is conducted. The use of the above technologies may, however, raise important legal, moral

[13] Mondaq (2024) *New UK legislation on security of IoT devices*. Available at: https://www.mondaq.com/uk/security/1444146/new-uk-legislation-on-security-of-iot-devices (Accessed: 3 September 2025).
[14] CR Advocates LLP (2023) *Cybercrimes in Kenya: Legal insights on IoT and digital security*. Available at: https://www.cradvocatesllp.com/cybercrimes-in-kenya-legal-insights-on-iot-and-digital-security (Accessed: 3 September 2025).

and other concerns. Top on the list of concerns is the infringement on constitutionally guaranteed freedoms and rights, such as the right to privacy under **Article 17**, the freedom of conscience, belief, and religion under **Article 19**, the freedom of expression under **Article 20,** and the right to dignity and protection from inhuman treatment under **Article 15** could all be affected.[15] If these technologies are not properly regulated, they could be used to secretly monitor people, limit their choices, control how they express themselves, or treat them in ways that go against human dignity.

The Zambian Constitution guarantees fundamental rights and freedoms under **Article 11**[16], including the right to life, liberty, freedom of conscience, expression, assembly, association, movement, protection from inhuman treatment, exploitation, and *privacy, including of one's property*. Further, **Article 17**[17] provides protection from unlawful search or entry of a person or their property. These rights are inalienable and are only subject to derogation in limited and necessary circumstances. However, with the emergence of IoB, there is a need to reassess whether these human rights were intended to include protection from virtual or internal bodily intrusion such as thought surveillance or mind suppression or whether the current legal framework requires reform or expansion to meet these unprecedented challenges.

While Zambia has enacted the **Data Protection Act**[18] to safeguard personal data, the legislation primarily addresses general data processing and lacks specific provisions for emerging technologies like IoT and IoB. Similarly, the **Cyber Security Act**[19]provides mechanisms for lawful interception of communications but does not explicitly regulate the unique challenges posed by IoB devices. The absence of targeted legal frameworks leaves a gap in addressing the nuanced issues related to bodily autonomy, mental privacy, and the ethical implications of integrating technology with human biology.

This dissertation critically examines the adequacy and appropriateness of Zambia's legal and regulatory framework in responding to and regulating the deployment of IoT and IoB

[15] Chapter 1 of the laws of Zambia
[16] The Constitution chapter 1 of the Laws of Zambia
[17] Ibid
[18] Act No. 3 of 2021
[19] Act No. 3 of 2025

technologies. It specifically focuses on the human rights implications of such technologies and evaluates whether constitutional protections such as the **right to privacy (Article 17)**,[20] **freedom of conscience**, and **right to liberty** can withstand the pressures introduced by new forms of digital intrusion.

1.3 RESEARCH OBJECTIVES

1. To examine the International legal framework Governing IoT and IoB Technologies

2. To examine the legal and regulatory framework governing Internet of Things, Internet of Beings and Human Rights in Zambia

3. To draw lessons from the United Kingdom and Kenya legal frameworks for IoT and IoB technologies

1.4 RESEARCH QUESTIONS

1. What international legal frameworks exist to regulate Internet of Things (IoT) and Internet of Beings (IoB) technologies, and how do they address the protection of human rights and privacy?
2. How adequate and appropriate is Zambia's legal and regulatory framework, including the Data Protection Act and Cybersecurity Act, in governing IoT and IoB technologies while safeguarding human rights such as privacy, freedom of conscience, and freedom of expression?
3. What lessons can Zambia learn from the United Kingdom and Kenya regarding the regulation of IoT and IoB technologies, and how can these lessons be applied to strengthen Zambia's legal and regulatory framework?

1.5 SIGNIFICANCE OF THE STUDY

This study is important because it helps people understand how new technologies like the Internet of Things (IoT) and the Internet of Beings (IoB) can affect their rights and freedoms in Zambia. As these technologies grow, they may be used in ways that touch on very personal areas of life, such as monitoring someone's thoughts or tracking their location. Right now, there are no clear laws in Zambia that explain what can or cannot be

[20] The Constitution chapter 1 of the Laws of Zambia

done with these technologies. This study shows why Zambia needs new laws to protect people's rights, especially the right to privacy, freedom of thought, and liberty.

1.6 LITERATURE REVIEW

The study by **Faith Mwafulirwa**[21] focuses primarily on the current Zambian legislation regarding the Internet of Things (IoT) and evaluates whether the Cyber Security and Cyber Crimes Act (CSCCA) and the Data Protection Act (DPA) adequately address the security and privacy issues introduced by IoT devices. Mwafulirwa's work looks at the existing laws and examines whether they protect users, with a particular emphasis on punishing offenders rather than preventing harm. In contrast, my study broadens the scope by not only addressing IoT but also introducing the emerging concept of the Internet of Beings (IoB), which extends IoT by involving living beings, including humans, in the digital ecosystem. My work explores the legal implications of both IoT and IoB and their impact on privacy, autonomy, and human rights in Zambia, while Mwafulirwa focuses only on IoT and its existing legislative framework. My study critically examines Zambia's legal framework for both IoT and IoB, identifying gaps and proposing comprehensive reforms. It emphasizes the impact on constitutional rights like privacy and freedom of conscience, going beyond Mwafulirwa's focus on IoT and comparative analysis.

In the 300th edition of EDRi-gram, **Mijatović and de Zwart**[22] discuss the future of digital rights, highlighting concerns about censorship, surveillance, and the role of technology in daily life. They emphasize the potential risks associated with neuro-implants and the monetization of personal data by public services. Their work underscores the challenges digital rights will face despite technological advancements. While their focus is on Europe, this study specifically examines the Zambian context, and seeks to address how IoT and IoB technologies intersect with local constitutional rights and the adequacy of existing legal frameworks.

[21] Faith Mwafulirwa (2023) The Internet of Things: Is The Zambian Law Adequate? A dissertation submitted in partial fulfillment of the requirements for the award of a Bachelor of Laws from the University of Lusaka

[22] EDRi-gram. (2015). 300 issues of EDRi-gram. Retrieved from https://www.wired.com/beyond-the-beyond/2015/05/300-issues-edri-gram

Michael Phillips[23] discusses the evolving legal challenges in the context of advancements in surveillance technology, noting that dramatic technological changes may lead to significant changes in legal interpretations of privacy. He emphasizes the need for laws to adapt to new technological realities. This study contributes to that discourse by examining Zambia's legal frameworks, such as the Data Protection Act and Cyber Security Act, to assess their effectiveness in addressing the challenges posed by IoT and IoB technologies

Zimba and Chembe[24]developed an IoT-based system to monitor water quality in Lusaka, aiming to detect contamination early and prevent disease outbreaks. Their work demonstrates how IoT can be applied in Zambia to address public health issues. However, they did not explore the legal or ethical implications of using such technology. In contrast, this study focuses on the legal challenges and human rights concerns associated with IoT and IoB technologies in Zambia.

Nicol[25] discusses how ICT policies are influenced by various stakeholders, including governments and private companies, and how these policies can sometimes conflict. While Nicol provides a general overview of ICT policy development, this study specifically examines Zambia's legal framework concerning IoT and IoB technologies and their impact on constitutional rights.

Souter [26]highlights the need for ICT policies to adapt to the convergence of different technologies and the importance of reviewing existing policies. While Souter emphasizes policy adaptation, this study delves into how Zambia's current laws address or fail to address the challenges posed by IoT and IoB technologies, particularly regarding individual rights.

Mwansa[27] reports on calls for the implementation of Zambia's national ICT policy to attract investors and transform the country into a knowledge-based society. While

[23] Michael Phillips (2013) A New Legal Theory for the Age of Mass Surveillance
[24] Zimba, S., & Chembe, C. (2022). Model for Water Quality Monitoring Based on Internet of Things. *Zambia ICT Journal*, 6(1), 44–51.
[25] Nicol, C. (2003). ICT Policy: A Beginner's Handbook. Association for Progressive Communications.
[26] Souter, D. (2009). The APC ICT Policy Handbook. Association for Progressive Communications.
[27] Mwansa, A. (2015, September 11). ICT policy will attract investors. Zambia Daily Mail.

Mwansa focuses on policy implementation for economic growth, this study concentrates on the adequacy of legal protections for individuals in the face of emerging technologies like IoT and IoB.

Polat[28] examines digital exclusion in Turkey, noting that technological advancements can exacerbate social inequalities if not addressed by inclusive policies. While Polat's work centers on access and inclusion, this study focuses on the potential infringement of rights due to the integration of IoT and IoB technologies in Zambia.

Patricia Boshe,[29] explored data privacy law reforms in Tanzania, focusing on the development of legal frameworks to protect personal data. While Boshe's work highlighted the progress in data protection legislation, it did not consider the specific challenges introduced by emerging technologies like IoT and IoB. This study seeks to address this gap by analyzing how such technologies impact constitutional rights and legal protections in Zambia.

Nchimunya Hanyama [30]in her study on internet access and usage in Zambia, Hanyama found that while Zambia has ICT policies like the ICT Act and the Electronic Communications and Transactions Act, there are issues with how these policies are put into action. She noted problems such as poor coordination between regulators and service providers, and a lack of clear information about internet policies. Her research focused on general internet access and the roles of different stakeholders. In contrast, this study looks specifically at newer technologies like the Internet of Things (IoT) and Internet of Beings (IoB), and how they might affect people's rights, especially concerning privacy and freedom of thought.

Makulilo[31] discussed how African countries, including Zambia, are adopting technology rapidly but often lack strong data protection laws. He highlighted that while technology is growing, laws to protect personal data are not keeping up, which can lead to misuse. His work looked at data privacy in general across Africa. This study, however, focuses on

[28] Polat, R. K. (2012). Digital exclusion in Turkey: A policy perspective. Government Information Quarterly, 29(4), 589–596

[29]Boshe, Patricia. (2016). Data Privacy Law Reforms in Tanzania. In Makulilo, A. B. (Ed.), African Data Privacy Laws. Springer.

[30] Hanyama, N. (2018). Policies and Legislation for Internet Access and Usage in Zambia. University of Zambia.

[31] Makulilo, A. B. (2016). African Data Privacy. Springer International Publishing.

specific technologies like IoT and IoB in Zambia and examines how current laws may not be sufficient to protect individuals from potential abuses related to these technologies.

Kugler [32]examined how data localization laws, which require data to be stored within a country, can impact trade in Africa. She argued that without proper data protection laws, countries might miss out on trade opportunities. Her research was centered on the economic effects of data laws. In contrast, this study is concerned with the legal and ethical implications of integrating technology with human bodies in Zambia, and how existing laws may not adequately address issues like mental privacy and bodily autonomy. Therefore, the gap lies in the limited attention given to how existing Zambian laws address or fail to address the unique challenges posed by IoB technologies, particularly in protecting human rights and ethical standards.

1.7 METHODOLOGY

This study uses a **qualitative research method**. This means that the study will not use numbers or statistics but will focus on understanding ideas, laws, and human rights by reading and analysing documents.[33] The aim is to look closely at Zambia's laws and see how they deal with new technologies like the Internet of Things (IoT) and the Internet of Beings (IoB).

The study will use **desk research**, which means reading different materials such as the Zambian Constitution, the Data Protection Act of 2021, and the Cyber Security and Cyber Crimes Act of 2021. It will also look at books, journal articles, reports, and online sources to understand how these laws work in practice and if they are enough to protect people's rights.

The study will also include a **comparative approach**, where it will look at how other countries are dealing with the same issues such as United Kingdom and Kenya. This will help show what Zambia can learn and what changes might be needed in its laws.

[32] Kugler, K. (2022). The Impact of Data Localisation Laws on Trade in Africa. Mandela Institute.

[33] Bowen, G. A. (2009). *Document analysis as a qualitative research method.* Qualitative Research Journal, 9(2), 27-40. https://studylib.net/doc/26180343/bowen-2009-document-analysis-as-a-qualitative-method

1.8 SCOPE OF THE STUDY

This study focuses on the legal and human rights issues connected to the use of IoT and IoB technologies in Zambia. It looks at how these technologies might be used, what risks they bring, and how current Zambian laws like the Constitution, the **Data Protection Act**,[34] and the **Cyber Security Act**[35]deal with them. The study also compares Zambia's legal approach to what other countries are doing and suggests what Zambia can do to catch up and protect its citizens.

1.9 ETHICAL CONSIDERATIONS

The researcher will make sure to obtain correspondence introducing her outlining that information collected is for academic purposes from the beginning in order to uphold high moral and ethical standards. The researcher promises to keep the data they collect secret and to use it only for academic study. Furthermore, the researcher shall credit the works of other authors in order to protect their copyright and free usage while using the OSCOLA referencing style.

[34] Act No. 3 of 2021
[35] Act No. 3 of 2025

CHAPTER TWO

THE INTERNATIONAL LEGAL FRAMEWORK GOVERNING IOT AND IOB TECHNOLOGIES

2.0 INTRODUCTION

This chapter examines the international legal framework that governs the use of Internet of Things (IoT) and Internet of Beings (IoB) technologies. It discusses how global instruments, such as the Universal Declaration of Human Rights (UDHR), the International Covenant on Civil and Political Rights (ICCPR), the European Union's GDPR, and the Budapest Convention on Cybercrime, provide rules to protect privacy, data, and human dignity. The chapter also examines African regional standards, particularly the Malabo Convention, which aims to harmonize data protection and cybersecurity across the continent. By analyzing these frameworks, the chapter shows how international and regional laws attempt to regulate emerging technologies, safeguard personal data, and uphold fundamental rights, even as new technologies create complex challenges for privacy, security, and human autonomy.

2.1 UNIVERSAL DECLARATION OF HUMAN RIGHTS (UDHR) 1948

The Universal Declaration of Human Rights (UDHR) is one of the first international documents to recognize the importance of privacy and dignity. **Article 12** [36]states that no one should face arbitrary interference with their privacy, family, home, or correspondence, nor should they suffer attacks on their honour and reputation. It also says that everyone has the right to protection by law against such interference or attacks.

Although the UDHR is not a legally binding treaty, it has become very influential. Many later treaties and national constitutions are built on its principles. It is also seen as part of customary international law, meaning that states are expected to respect it even if they did not formally adopt it. For IoT and IoB technologies, **Article 12** [37]provides a moral and legal foundation for protecting people from invasive monitoring, data collection without

[36] United Nations. (1948). *Universal Declaration of Human Rights (UDHR)*. Adopted by the UN General Assembly Resolution 217 A (III). Retrieved from https://nations-united.org/Universal_Declaration_Of_Human_Rights/Articles_Human_Rights/Articles_12_Human_Rights_Universal_Declaration_Nations_United_Twelve.htm

[37] Ibid

consent, or other forms of privacy breaches. Even though the UDHR does not mention digital or biological technologies, its spirit clearly applies to them, because the principle of protecting personal life and dignity is universal.

2.2 INTERNATIONAL COVENANT ON CIVIL AND POLITICAL RIGHTS (ICCPR) 1966

The ICCPR takes the ideas in the UDHR further and makes them legally binding for states that ratify it. **Article 17(1)** [38]protects people from arbitrary or unlawful interference with their privacy, family, home, or correspondence, and from unlawful attacks on their honour and reputation. **Article 17(2)** [39]ensures that everyone has the right to legal protection if these rights are violated. This means governments must pass laws and provide remedies when privacy is invaded.

Other articles in the ICCPR are also very relevant to IoT and IoB. **Article 18** protects freedom of thought, conscience, and religion. This becomes important when considering technologies that could monitor or influence people's inner thoughts or beliefs. **Article 19** protects freedom of expression, which could be threatened if technologies limit how people share their ideas or feelings. **Article 7** [40]prohibits cruel, inhuman, or degrading treatment. If IoB technologies are misused to manipulate minds, cause harm to dignity, or subject people to degrading experiences, such misuse could fall under this prohibition. Taken together, the ICCPR creates stronger obligations than the UDHR. It requires states to actively protect individuals from privacy violations and ensure dignity and freedom are respected, even as new technologies like IoT and IoB emerge.

2.3 THE ROLE OF GDPR IN REGULATING PERSONAL DATA

The General Data Protection Regulation (GDPR) is one of the strongest data protection laws in the world. It was introduced in 2018 by the European Union and applies not only within the EU but also to organizations outside the EU that deal with data of EU residents. This makes GDPR global in its effect. It sets out rules on how personal data should be

[38] United Nations. (1966). *International Covenant on Civil and Political Rights (ICCPR)*. Adopted by UN General Assembly Resolution 2200A (XXI). Retrieved from https://legal.un.org/avl///ha/iccpr/iccpr.html
[39] United Nations. (1966). *International Covenant on Civil and Political Rights (ICCPR)*. Adopted by UN General Assembly Resolution 2200A (XXI). Retrieved from https://legal.un.org/avl///ha/iccpr/iccpr.html
[40] Ibid

collected, used, stored, and shared. Personal data means any information that can identify a person, such as their name, email, address, or health details.[41]

A central rule under GDPR is **Article 6**,[42] which explains when processing personal data is lawful. Processing is only allowed if it meets certain conditions. For example, data can be processed if the person has given clear consent, if it is necessary for a contract, if it is needed to meet a legal obligation, if it protects vital interests like health or safety, if it is carried out for a public task, or if it is needed for the controller's legitimate interest provided it does not override the person's rights. These conditions are important for IoT and IoB because such technologies collect large amounts of data, often automatically, and need a lawful basis to do so.[43]

Another key feature of GDPR is the idea of **data protection by design and by default**. This means that devices, systems, or apps must be designed with privacy in mind from the very beginning. For example, an IoT device such as a smart watch should not collect more data than is necessary and should provide strong security from the start. By default, only the minimum amount of personal data needed for the service should be processed. This principle protects users because it prevents unnecessary data collection and reduces the risk of misuse.

GDPR also strengthens the rights of individuals. It gives people more control over their personal information. A person has the right to access their data and know how it is being used. They can ask for corrections if their data is inaccurate, and they can request deletion of their data in certain situations, also known as the "right to be forgotten." People also have the right to restrict processing, to object to certain uses of their data, and to move their data to another provider through the right to data portability. Importantly, when decisions are made automatically, such as by artificial intelligence systems, GDPR gives individuals the right to request human involvement and explanations.[44]

---

[41] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1.

[42] Ibid

[43] Ibid

[44] European Commission, 'Data Protection in the EU' (European Commission, 2023) https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_en accessed 18 September 2025.

2.3.1 GDPR and Its Impact on IoT and IoB

IoT and IoB technologies raise special concerns because they often collect very sensitive information, especially health and biometric data. For example, a smart medical implant or a fitness tracker constantly records details about the user's body and health. Under GDPR, this type of data falls into a special category that requires stricter protection. In most cases, the person's **explicit consent** is required before such data can be processed. Organizations must also put in place strong safeguards, like encryption and strict access controls, to protect the data.

Another important rule under GDPR is about **cross-border data transfers**. Many IoT devices send information to servers located in different countries. GDPR requires that if personal data is transferred outside the EU, it must still receive the same level of protection. This is usually achieved through mechanisms such as adequacy decisions, standard contractual clauses, or binding corporate rules. This ensures that individuals' data is not put at risk when moved across borders.[45]

GDPR also puts obligations on organizations that make or use IoT and IoB devices. They must carry out **data protection impact assessments** if their data processing is likely to pose high risks to people's rights. For example, a company making IoB devices like smart pacemakers must carefully examine the risks to privacy, security, and safety before releasing the product. Supervisory authorities in EU countries can check compliance and impose heavy fines if the rules are not followed. These fines can be up to 20 million euros or 4% of global annual turnover, whichever is higher.[46]

The influence of GDPR goes far beyond the EU. Many countries have passed or updated their own data protection laws to align with GDPR principles. This has made GDPR a global standard in privacy protection.[47] For IoT and IoB technologies, this means that

[45] GDPR.eu, 'What is GDPR, the EU's new data protection law?' (GDPR.eu, 2023) https://gdpr.eu/what-is-gdpr/ accessed 18 September 2025.

[46] European Commission, 'Data Protection in the EU' (European Commission, 2023) https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_en accessed 18 September 2025.

[47] European Data Protection Board, 'Guidelines on Data Protection by Design and by Default' (EDPB, 2020) https://edpb.europa.eu/ accessed 18 September 2025.

companies around the world must consider GDPR rules if they want to sell to EU residents or handle their data.[48]

2.4 BUDAPEST CONVENTION ON CYBERCRIME

The Budapest Convention on Cybercrime, also known as Convention 185, is the first international treaty designed to address crimes committed through the internet and other digital networks. It was adopted by the Council of Europe in 2001 and entered into force in 2004. Although it was developed by European countries, its influence is global because many non-European states, such as the United States, Japan, and South Africa, have also joined it. This gives the Convention a wide and binding nature for all member states that have ratified it. States that are not parties may also align their domestic laws with its standards to improve cooperation in fighting cybercrime.

The Convention aims to harmonize national laws, improve investigation techniques, and strengthen international cooperation against cybercrime. It sets out a legal framework that defines offences such as illegal access to computer systems, data interference, system interference, misuse of devices, and computer-related fraud or forgery. It also requires member states to criminalize these offences under their domestic laws. This harmonization ensures that cybercriminals cannot escape prosecution simply by operating across borders.

Article 2 of the Convention[49] focuses on **illegal access**. It requires countries to criminalize accessing computer systems without permission. In practice, this means that if someone hacks into an IoT device, like a smart thermostat, or an IoB device, such as a wearable health monitor or a medical implant, without authorization, it is considered a crime. This article helps protect the devices themselves and the sensitive information they collect, ensuring that individuals' personal and health data are not accessed unlawfully.

Article 3[50] addresses **illegal interception** of communications. Many IoT and IoB devices constantly send and receive data. **Article 3** makes it a criminal offense to intercept these

[48] Information Commissioner's Office (ICO), 'Guide to the UK General Data Protection Regulation (UK GDPR)' (ICO, 2023) https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/ accessed 18 September 2025.

[49] Ibid

[50] Council of Europe, *Convention on Cybercrime* (Budapest, 23 November 2001) ETS 185, https://rm.coe.int/1680081561 accessed 18 September 2025.

communications without consent. For example, if a hacker captures information sent from a heart monitor to a healthcare provider, or intercepts signals from a home security system, it would be illegal. This provision protects both privacy and the integrity of the data transmitted through these devices.

Article 4 covers **data interference**, which is the illegal alteration, deletion, or suppression of data. It obliges countries to make it a crime to intentionally interfere with data stored or processed by a computer system. For IoT and IoB, this could include tampering with health records collected by a wearable device, changing data sent by a smart home appliance, or disabling the functionality of a medical implant. By criminalizing these actions, the Convention ensures that the data collected by these technologies remains reliable and accurate.[51]

Article 5[52] deals with **system interference**. This refers to actions that disrupt or damage computer systems. The Convention requires countries to make it illegal to intentionally impair the normal functioning of a system. In the context of IoT and IoB, this could mean cyberattacks that shut down smart home devices, disable industrial IoT equipment, or disrupt medical implants. The provision ensures that systems are protected not only from unauthorized access but also from interference that could endanger users or compromise operations.[53]

Article 6[54] is about the **misuse of devices**. It mandates that producing, distributing, or possessing tools or software designed to commit cybercrimes should be criminalized. This is very relevant for IoT and IoB, as hackers may use specialized software or devices to exploit vulnerabilities.[55] For example, creating a program that can remotely control pacemakers or manipulate smart appliances would be illegal under this article. The provision addresses not just the crime itself but also the tools used to commit it, making it harder for cybercriminals to operate.

Relevance of the Budapest Convention to IoT and IoB

[51] Ibid
[52] Ibid
[53] Ibid
[54] Ibid
[55] Council of Europe, *Convention on Cybercrime* (Budapest, 23 November 2001) ETS 185, https://rm.coe.int/1680081561 accessed 18 September 2025.

The Budapest Convention on Cybercrime is important for both IoT and IoB technologies because these devices collect and transmit sensitive data and can affect a person's health, safety, and privacy. By creating clear legal rules against cyberattacks, the Convention helps countries protect users, devices, and the information they hold.

The Convention addresses the main cybercrimes that threaten IoT and IoB through its core provisions. It criminalises illegal access under **Article 2**[56], illegal interception under Article 3, data interference under **Article 4,** [57]system interference under Article 5, and the misuse of cybercrime tools under **Article 6.** [58]These rules mean that actions such as hacking a smart home system or tampering with a wearable medical device are punishable offences.

A major strength of the Convention is its focus on international cooperation because cyberattacks often cross borders. It enables countries to share evidence, coordinate investigations, and extradite offenders, closing legal gaps that criminals might exploit. The Convention is also flexible and can be applied to new and emerging cyber threats, ensuring continued protection as IoT and IoB technologies evolve.

2.5 MALABO CONVENTION

The African Union Convention on Cyber Security and Personal Data Protection, also known as the *Malabo Convention*, was adopted in 2014. It is the first continental treaty in Africa that directly addresses issues of cyber security, electronic transactions, and the protection of personal data. Its goal is to create a common legal framework for African states so that they can handle new challenges that come with digital technologies.[59]

The Convention has several chapters, but one of the most important is **Chapter II**, which focuses on data protection. It requires states to adopt laws that protect people's personal data and make sure that data is collected and processed fairly, lawfully, and for clear purposes. It also gives individuals the right to know how their personal data is used and

[56] Council of Europe, Convention on Cybercrime (Budapest, 23 November 2001) ETS 185, https://rm.coe.int/1680081561 accessed 18 September 2025.
[57] Ibid
[58] Ibid
[59] Media Defence. (2021). The African Union's Malabo Convention and data protection in Africa. Retrieved from https://www.mediadefence.org

the ability to challenge misuse. For example, **Article 8**[60] requires that personal data must be collected for specific, explicit, and legitimate purposes and not processed in ways that are incompatible with those purposes. **Article 9**[61] further requires that data must be adequate, relevant, and not excessive in relation to the purposes for which it is collected. The Malabo Convention also sets out principles of consent and transparency. **Article 13**[62] provides that personal data can only be processed if the individual has given their free, specific, and informed consent. This is especially important when dealing with technologies like the Internet of Things (IoT) and Internet of Beings (IoB), where sensitive data such as health information, biometric identifiers, or even brain-related signals might be collected. Without proper consent, such processing would violate the Convention.

2.5.1 Relevance of the Malabo Convention to IoT and IoB

The Malabo Convention is very relevant to new technologies like IoT and IoB because of its emphasis on consent, lawful use of data, and protection against misuse. For example, if a person uses a wearable device that monitors their heartbeat, or a brain-computer interface that collects neural signals, **Article 9**[63] would require that their data cannot be collected secretly or used for purposes they did not agree to. This supports the right to privacy and bodily autonomy.

The Convention also sets obligations on states. **Article 10** [64]requires states to establish an independent data protection authority to make sure that the rules are respected. This is important because laws alone are not enough there must be institutions that can monitor companies, government agencies, or any other actors that collect and process personal data. For Zambia, which already has the **Data Protection Act of 2021**, aligning with the Malabo Convention can strengthen national systems and bring them closer to regional standards.

---

[60] African Union. (2014). *African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention).* Adopted in Malabo, Equatorial Guinea, 27 June 2014. Retrieved from https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection

[61] Ibid

[62] Ibid

[63] African Union. (2014). *African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention).* Adopted in Malabo, Equatorial Guinea, 27 June 2014. Retrieved from https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection

[64] Ibid

Another important part is **Article 25**,[65] which criminalizes violations of personal data protection rules. This includes collecting or processing data unlawfully or failing to secure it properly. For IoT and IoB, this is crucial because a breach of health or neural data could cause serious harm, including loss of privacy, discrimination, or manipulation of personal behaviour.

While the Malabo Convention provides a strong foundation, it still faces challenges. One problem is that not many African countries have ratified it, so its impact is limited. Another challenge is that the Convention does not explicitly mention IoT or IoB technologies, since these were still developing when it was drafted. However, its broad language about personal data and protection of individuals makes it flexible enough to be applied to new technologies.

For Zambia, the Malabo Convention offers a chance to expand its legal framework beyond the current **Data Protection Act** [66]and **Cyber Security and Cyber Crimes Act**[67]. By fully embracing the Convention's provisions such as the requirements on consent, clear purposes for data processing, independent oversight, and criminal liability for misuse Zambia can better protect its citizens from the risks of IoT and IoB technologies.

2.6 CONCLUSION

International and regional legal frameworks play a crucial role in regulating IoT and IoB technologies and protecting human rights. Instruments like the UDHR, ICCPR, GDPR, and Budapest Convention provide clear rules on privacy, consent, data security, and protection from abuse, while the Malabo Convention offers guidance for African states, including Zambia, to strengthen national laws and oversight. Together, these laws aim to ensure that emerging technologies are used responsibly and ethically, protecting individuals from privacy violations, misuse of personal data, and potential harm to bodily and mental autonomy. As IoT and IoB continue to develop, these frameworks provide a foundation for adapting national laws to meet new technological challenges while safeguarding fundamental human rights.

[65] Ibid
[66] Act No. 3 of 2021
[67] Act No. 3 of 2025

CHAPTER THREE

THE LEGAL AND REGULATORY FRAMEWORK GOVERNING INTERNET OF THINGS, INTERNET OF BEINGS AND HUMAN RIGHTS IN ZAMBIA

3.0 INTRODUCTION

The development of the Internet of Things (IoT) and the Internet of Beings (IoB) presents both opportunities and risks. These technologies allow devices, systems, and even human biological functions to be connected and monitored digitally. While they can bring improvements in healthcare, communication, business efficiency, and governance, they also raise concerns about the protection of human rights. In Zambia, the Constitution guarantees fundamental rights and freedoms under **Article 11**, such as the right to privacy, dignity, liberty, and freedom of expression. However, IoT and IoB technologies introduce new risks of surveillance, control, and intrusion that existing laws may not fully address. This chapter examines Zambia's constitutional, statutory, and regulatory framework governing IoT, IoB, and human rights, and assesses whether these protections are sufficient in the digital age.

3.1 CONSTITUTION OF ZAMBIA AND THE PROTECTION OF HUMAN RIGHTS IN THE AGE OF IoT AND IoB

The Constitution of Zambia is the supreme law of the land. **Article 1(1)** [68]makes it clear that the Constitution overrides all other written laws, customary laws, and customary practices, and that any law inconsistent with its provisions is void to the extent of the inconsistency. This principle was well explained in ***Thomas Mumba v The People*** [69]where Justice D.K. Chirwa held that because the Constitution is supreme, all laws derive their validity from it, and any law that conflicts with it is null and void unless the Constitution itself is amended. This shows that the Constitution forms the foundation of all rights and freedoms in Zambia and acts as the highest safeguard against any form of abuse.

[68] The Constitution of Zambia, Act No. 2 of 2016.
[69] (1984) ZR, 38

The Bill of Rights in Part III of the Constitution sets out the fundamental rights and freedoms of every person. **Article 11**[70] provides that these include the right to life, liberty, security, privacy, dignity, freedom of conscience, freedom of expression, freedom of movement, and protection from inhuman treatment. These rights are inalienable and may only be limited under necessary and lawful circumstances. However, with the rapid growth of the Internet of Things (IoT) and the Internet of Beings (IoB), questions arise as to whether the Constitution is strong enough to protect citizens from new forms of intrusion into their private and even biological lives.[71]

The right to **privacy** is of particular importance. **Article 17** [72]protects individuals against unlawful search or entry of their person or property. Traditionally, this was understood in terms of physical searches of homes, offices, or possessions. In the digital age, however, IoT devices such as smartphones, smart watches, and home security systems collect vast amounts of personal data, often without the clear knowledge of users. IoB technologies go further by connecting directly with human biology, for example through brain-computer interfaces, biometric implants, or wearable devices that track emotions and thoughts. The question arises whether **Article 17** [73]can be interpreted to include this new type of intrusion, sometimes called “mental privacy.” If not, then the constitutional guarantee may fall short of protecting people in the digital era.

The Constitution also provides for the right to **dignity and protection from inhuman treatment** under **Article 15**[74]. Dignity is a central value in a democratic society, as it ensures that all individuals are treated with respect and humanity. IoB devices, if misused, could threaten this right by interfering with human bodily functions or manipulating emotions and thoughts. For example, an implant used for medical treatment could also be exploited to control a person’s decisions or limit their freedom of thought. If used

[70] Chapter 1 of the Laws of Zambia
[71] Smith, J. (2020). "The Intersection of Privacy Rights and Data Protection: A Comparative Analysis." Journal of Comparative Law, 15(2), 123-145.
[72] Chapter 1 of the Laws of Zambia
[73] Ibid
[74] Ibid

coercively, such practices would amount to degrading or inhuman treatment, directly conflicting with the protections under **Article 15.**

Another important right is the **freedom of conscience, belief, and religion** under **Article 19**. This guarantees every person the liberty to hold their own beliefs and convictions without interference. The rise of IoB technologies, which may be able to monitor or even influence brain activity, creates the risk that the state or private actors could intrude into the inner sphere of human thought. This could undermine freedom of conscience by shaping or suppressing people's beliefs, which would directly violate **Article 19**[75]. The Constitution, however, remains silent on whether such "internal surveillance" is included within its scope, leaving a legal gap that could be exploited.

The right to **freedom of expression** is also guaranteed under **Article 20.** [76]This right allows individuals to freely communicate ideas and opinions without interference. In the digital age, much of this expression takes place through IoT devices such as mobile phones, social media platforms, and smart communication systems. If these devices are monitored, censored, or controlled, it would directly affect the ability of individuals to express themselves. IoB technologies further complicate matters, as they could be used to track not only what people say but also what they intend to say or feel. Such interference would strike at the very heart of freedom of expression.[77]

Despite the strong wording of the Constitution, it is clear that it was drafted in an era when technologies such as IoT and IoB were not imagined. The Constitution does not expressly protect "mental privacy" or regulate how far digital and biological surveillance may go. As a result, there is a need for rethinking or expanding constitutional protections to ensure that they remain relevant in the digital age. If left unchanged, there is a risk that constitutional rights may be weakened by technologies that operate beyond the traditional definitions of privacy, dignity, and liberty.

[75] Chapter 1 of the Laws of Zambia
[76] Ibid
[77] Jones, A., & Patel, R. (2019). "Protecting Privacy in the Digital Age: Legal Challenges and Solutions." International Journal of Law and Technology, 8(3), 211-230.

Importantly, the Constitution provides mechanisms for the enforcement of rights. **Article 28 and Article 128** [78]give the High Court jurisdiction to hear and determine matters relating to the violation of fundamental rights. This gives the courts the power to reinterpret rights in a modern way that includes digital and biological threats. In addition, **Article 230**[79]establishes the Human Rights Commission, with the mandate to promote and protect human rights, investigate complaints, and monitor compliance by state organs. This body could play a crucial role in ensuring that rights are protected in relation to IoT and IoB.

In line with Zambia's obligations under international human rights law, the state is also required to enact and enforce legislation that strengthens constitutional rights. While laws such as the Data Protection Act and the Cyber Security and Cyber Crimes Act have been enacted, they still fall short in addressing the unique challenges posed by IoB technologies. Without reforms, the existing protections may prove inadequate, and citizens could be left vulnerable to violations of privacy, dignity, and conscience in ways that were not foreseen by the framers of the Constitution.

3.2 THE DATA PROTECTION ACT AND ITS GAPS IN REGULATING IOT AND IOB

The Data Protection Act was made to protect how personal data is collected, stored, transmitted, and used. It applies to any processing of personal data that is done fully or partly by automated means. This means it can be used to regulate IoT devices because such devices depend on automated data processing. However, the Act does not apply to data processed by an individual for their personal use. **Section 3 of the Act**[80] mentions this but does not clearly define what "personal use" means. Because of this, it is not clear how far the law applies when people use personal devices like smart home systems or health wearables that collect information about others. This lack of clarity makes it difficult to know when the law applies and when it does not.

3.2.1 Key Principles of Data Processing

[78] The Constitution of Zambia, Act No. 2 of 2016.
[79] Ibid
[80] Data Protection Act No. 3 of 2021

The Act sets out principles that must be followed whenever personal data is processed. **Section 12(1)**[81] states that data controllers and processors must process data lawfully, fairly, and transparently. Data must be collected for clear and legitimate reasons and only what is necessary should be processed. It must also be accurate, updated, and erased if it is wrong. Data should not be kept longer than needed and must be protected against loss, misuse, or unauthorized access.

These principles are important for IoT and IoB technologies because devices connected to the internet collect large amounts of information automatically. For example, a smart watch records heart rate, sleep, and movement data. If this data is not protected or deleted in time, it can expose users to privacy risks. However, the law does not directly talk about new kinds of data created by IoB devices, such as brain activity or emotional patterns. These types of data are very personal and need stronger protection, yet they are not specifically mentioned in the Act.[82]

3.2.2 Grounds for Processing Personal Data

Section 13 of the Data Protection Act[83] sets out the legal reasons that allow personal data to be processed. Data can only be collected and used if it falls under one of these lawful grounds. These include when the person gives consent, when processing is needed to perform a contract, to comply with a legal duty, to protect someone's vital interests, to perform a public task, or to pursue the legitimate interests of the data controller. These rules are similar to those found in the European Union's General Data Protection Regulation (GDPR), which also requires a clear legal basis for data processing. The aim of these provisions is to make sure that people's information is only used for lawful and fair purposes.

Although consent is one of the main lawful grounds under **Section 13(a),** [84]it is often not properly understood by users of IoT and IoB devices. Most people agree to terms and conditions without reading them because they are long and filled with technical language.

[81] Data Protection Act No. 3 of 2021
[82] Ibid
[83] Ibid
[84] Ibid

This means that many users do not fully understand what they are agreeing to. For example, someone using a fitness tracker may think they are only sharing their exercise data, but the device might also collect sensitive medical information such as heart rate, blood pressure, or sleep patterns. This makes the consent less meaningful because it was not given with full knowledge of what data is being collected and how it will be used. True consent should be clear, specific, and freely given, but in most cases involving IoT and IoB, it is broad and general.

Therefore, **Section 13(b)(v)**[85] allows data controllers to process personal data based on their "legitimate interests." While this can be useful for running businesses, it is also open to misuse. Companies and government agencies may claim a legitimate interest even when their activities invade personal privacy. For example, a company might argue that it has a legitimate interest in tracking user behavior through connected devices to improve its services, even if this leads to excessive data collection. In the IoB space, where devices monitor personal health or emotional patterns, such justification can be dangerous. Without clear limits, "legitimate interest" can be used as an excuse to collect sensitive data without proper safeguards.

3.2.3 Rights of Data Subjects

Sections 58 to 65 of the Act[86] give people, known as data subjects, several rights over their data. These include the right to know if their data is being processed, to access that data, and to understand why it is being used. **Section 59** gives the right to correct inaccurate data, while **Section 60** allows a person to request the deletion of their data in certain cases. **Section 61** gives the right to object to data processing, and **Section 62** says that no one should be affected by a decision based only on automated processing, such as profiling, if it has legal or significant effects.[87]

These rights are very important in the IoT and IoB environment. For example, a person using a medical implant that collects health data should have the right to see what information is stored, delete it when no longer needed, or object to its use. However,

[85] Data Protection Act No. 3 of 2021
[86] Ibid
[87] Ibid

many IoT and IoB devices work in the background and users may not even know that their data is being collected. This makes it hard for people to exercise their rights because they cannot act on what they do not know. Although the law gives strong rights, putting them into practice is still difficult.

3.2.4 Enforcement and Penalties

The Act sets penalties to make sure that those who handle data follow the rules. **Section 18**[88] states that a company that breaks the law may be fined up to one hundred million penalty units or two percent of its annual turnover, whichever is higher. A natural person can be fined up to one million penalty units or imprisoned for up to five years, or both. These penalties are meant to discourage misuse and encourage responsible data handling.

However, enforcing these penalties in the IoT and IoB space is not easy. Many of the devices used in Zambia are made and controlled by companies in other countries. The Data Protection Commissioner may find it difficult to take action against foreign companies that process Zambian citizens' data outside the country. Also, while the Act recognizes sensitive data, it does not mention certain types such as neurological or emotional data. This omission weakens protection of mental privacy and bodily autonomy, both of which are vital for IoB technologies.

3.2.5 Key Issues under the Data Protection Act

From the above provisions, several issues stand out. First, Section 3 does not clearly explain what "personal use" means, making the law's scope uncertain for people using personal IoT devices. Second, the principles in Section 12(1) are strong in theory but do not deal directly with complex IoB data like brain activity. Third, the lawful grounds in Section 13 are easily misused because consent is often uninformed and "legitimate interest" can be stretched too far. Fourth, although Sections 58 to 65 give people control over their data, it is hard for them to exercise these rights when data is collected secretly. Finally, enforcement under Section 18 faces real challenges due to foreign companies and the lack of clear rules on sensitive IoB data. while the Data Protection Act provides a

[88]Data Protection Act No. 3 of 2021

good foundation for protecting personal data, it still leaves several gaps in the area of IoT and IoB technologies. These gaps must be addressed to ensure full protection of privacy, security, and bodily integrity in the digital age.

3.3 CYBER SECURITY ACT NO. 3 OF 2025

The Cyber Security Act No. 3 of 2025 is Zambia's most recent law that deals with the regulation of cyber activities, interception of communications, and monitoring of digital systems. It repealed and replaced the Cyber Security and Cyber Crimes Act of 2021. The new Act was introduced to strengthen cyber resilience, create better mechanisms for lawful interception, and ensure that interception is only done through one centralized facility known as the Central Monitoring and Coordination Centre under **Section 21**[89].[90] This Centre acts as the sole facility through which all lawful interceptions must be carried out, and it is managed by the division responsible for government communications.

3.3.1 Offences Relating to Unauthorised Interception

In line with our topic and statement of the problem, the Act directly affects how technologies such as the Internet of Things (IoT) and the Internet of Beings (IoB) are handled when it comes to issues of surveillance, monitoring, and privacy. For instance, **Section 22** [91]makes it a crime for any person to knowingly intercept, attempt to intercept, or use devices to intercept communications without lawful authority. Offenders can face up to ten years imprisonment or a fine not exceeding one million penalty units, or both. Similarly, **Section 23** [92]prohibits the unauthorized use, manufacture, or possession of interception devices. This is important because IoT and IoB technologies generate highly sensitive data, including geolocation and even health or brainwave data, and if interception devices are abused, the rights of citizens to privacy under **Article 17** of the Constitution would be at risk.

3.3.2 Judicial Oversight and Emergency Interception

[89] Act No. 3 of 2025
[90] Ibid
[91] Ibid
[92] Ibid

The Act also introduces safeguards to ensure that interception is done with oversight from the courts. **Section 29** [93]provides that a law enforcement officer can only intercept communications if they obtain an interception order from a judge. The order can require service providers to intercept and retain specific communications or even allow installation of interception devices on premises. Such orders must be based on reasonable grounds that the communication relates to an offence or to locating a suspect. The order lasts for three months but can be renewed once for another three months. While this mechanism provides some judicial oversight, it still raises concerns because of the breadth of power given to law enforcement. If misused, it could expose personal data from IoT devices like smart home systems or IoB implants, thereby threatening freedoms such as dignity **(Article 15),** liberty **(Article 11),** and freedom of expression **(Article 20**).[94]

Another important feature of the Act is **Section 30**, which allows law enforcement officers to request oral interception of communications in emergencies, such as preventing bodily harm, death, or serious damage to property. While this provision is aimed at protecting life and public safety, it bypasses prior judicial authorization, allowing interception first with judicial confirmation only after the fact. This creates a risk of abuse, especially when IoB devices collect intimate data such as medical information or thought patterns.

3.3.4 Protection of Geolocation and Monitoring Restrictions

The Act also regulates the acquisition and use of geolocation information under **Section 31.**[95] It makes it unlawful for any person to intentionally acquire or disclose someone's geolocation data without their consent. This is crucial in the IoT and IoB environment where location tracking is common, whether through wearable devices, vehicles, or medical implants. However, although this protection is a positive step, the enforcement of such provisions remains weak in practice.

[93] Act No. 3 of 2025
[94] Chapter 1 of the Laws of Zambia
[95] Act No. 3 of 2025

Furthermore, **Section 37** [96]prohibits random monitoring of communications. This means that authorities and service providers cannot monitor communications unless it is done lawfully, for example, through service quality checks or with proper authorization. This provision is important because it reduces the chances of mass surveillance of IoT and IoB users, which would otherwise threaten constitutional freedoms.

Despite these measures, the Act still leaves serious gaps in protecting bodily autonomy and mental privacy. The law speaks broadly about communication interception but does not provide specific protection for IoB-generated data, such as neural or biometric information, which directly relates to human dignity and liberty. In line with the statement of the problem, this means that while the Act creates a legal framework for interception, it does not fully address the emerging risks that IoB presents, such as thought surveillance or manipulation of human biological functions.

3.4 THE CYBER CRIMES ACT NO. 4 OF 2025

The **Cyber Crimes Act No. 4 of 202**5 is Zambia's most recent law aimed at combating cyber threats, protecting data, and regulating the use of computer systems. This Act introduces a wide range of offences to deal with cybercrime and strengthens penalties for misuse of technology. Its provisions are important when examining the Internet of Things (IoT) and the Internet of Beings (IoB), as both rely on computer systems, networks, and data flows that could be misused if not properly regulated.

3.4.1 Offences Relating to Unauthorised Access and Interference

Under **Section 3(1)**,[97] it is an offence for a person to intentionally and without lawful authority access or monitor another person's computer system. This provision is relevant to IoT and IoB because devices such as smart home assistants or implanted medical devices can be hacked, allowing strangers or even state agencies to monitor private lives. If misused, this could violate the constitutional right to privacy under **Article 17**.[98] The Act

[96] Act No. 3 of 2025
[97] Act No. 4 of 2025
[98] Ibid

criminalises such acts and prescribes imprisonment of up to five years, showing recognition of the seriousness of digital intrusions.

Similarly, **Section 4**[99] prohibits interference with another person's data or computer system, including destroying, altering, or blocking lawful use of information. For IoB, this is critical because interference could mean tampering with health devices, neural implants, or biometric systems, potentially endangering human life. A malfunction caused by cyber interference could amount to inhuman treatment, contrary to **Article 15**[100] of the Constitution, which protects individuals from degrading or harmful treatment.

3.4.2 Protection Against Unauthorised Disclosure and Surveillance

The Act also addresses unauthorised disclosure of sensitive data. **Section 5**[101] makes it an offence to intentionally communicate or transmit information relating to critical infrastructure without authority. In the IoB environment, critical infrastructure may include medical data, biometric identifiers, or brain-computer interface codes. If exposed, such information could be used to manipulate people's bodies or minds, raising questions about dignity and liberty under **Article 11**.[102]

Another important safeguard is found in **Section 10**,[103] which prohibits recording private conversations without the knowledge of the parties involved. IoT and IoB devices often have built-in microphones and sensors that can capture private conversations. Without proper regulation, these technologies could be used to secretly monitor individuals, undermining the right to freedom of expression under **Article 20**.[104]

3.4.3 Cyber Extortion, Child Protection, and Remaining Gaps

The Act also criminalises cyber extortion, identity-related crimes, and child exploitation through digital systems (**Sections 12–18**). These provisions are vital because IoT and IoB technologies could be exploited to blackmail individuals by threatening to reveal

[99] Act No. 4 of 2025
[100] Chapter 1 of the Laws of Zambia
[101] Act No. 4 of 2025
[102] Chapter 1 of the Laws of Zambia
[103] Act No. 4 of 2025
[104] Chapter 1 of the Laws of Zambia

private biological or mental data. In cases involving children, IoT-connected devices like tablets or online platforms could be misused for grooming and trafficking, which would directly endanger children's rights under **Article 24** of the Constitution.[105]

Despite these protections, challenges remain. The Act does not yet make a clear distinction between ordinary data and highly sensitive biological or neurological data generated by IoB devices. As such, while it criminalises unlawful access, interference, and disclosure, it does not explicitly address the special risks of mind surveillance or bodily manipulation. This gap means that although the law provides a stronger framework than before, it may not fully safeguard the new dimensions of human rights at risk in the IoT and IoB age.

3.5 CONCLUSION

From the discussion, it is clear that Zambia has made important progress in regulating digital technologies through its Constitution and recent laws such as the **Data Protection Act, the Cyber Security Act No. 3 of 2025, and the Cyber Crimes Act No. 4 of 2025**. These laws address issues of privacy, interception of communication, data protection, and cybercrime, and they create penalties to discourage abuse. They also reflect Zambia's recognition of the need to protect fundamental rights in the digital environment. However, the rise of IoT and IoB exposes weaknesses in the current framework, particularly the lack of specific protection for sensitive biological and neurological data. Rights such as mental privacy, dignity, and freedom of thought are not yet fully safeguarded against the risks posed by IoB technologies, which can directly connect with and even influence human minds and bodies. This means that while Zambia's legal system is moving in the right direction, it still falls short of fully protecting citizens in the new digital era. Stronger reforms and clearer safeguards will be required if the country is to ensure that technological progress does not come at the expense of fundamental human rights.

[105] Ibid

CHAPTER FOUR

LESSONS FROM THE UNITED KINGDOM AND KENYA LEGAL FRAMEWORKS FOR IOT AND IOB TECHNOLOGIES

4.0 INTRODUCTION

This chapter examines at how the United Kingdom and Kenya have developed strong legal systems to manage and protect the use of Internet of Things (IoT) and Internet of Bodies (IoB) technologies. These two countries have built legal frameworks that focus on privacy, cybersecurity, and human rights in the digital age. The United Kingdom uses laws such as the Data Protection Act 2018, the UK GDPR, and the Computer Misuse Act 1990, which provide detailed rules for handling personal and sensitive information. Kenya, on the other hand, has created a modern data protection and cybercrime framework through the Data Protection Act 2019 and the Computer Misuse and Cybercrimes Act 2018. Both systems show how the law can keep up with rapid technological change by promoting safety, transparency, and accountability. By studying these two countries, Zambia can draw practical lessons on how to strengthen its own legal protections for emerging technologies, especially those that collect personal and biological data.

4.1 THE UNITED KINGDOM LEGAL FRAMEWORK FOR IOT AND IOB TECHNOLOGIES

4.1.1 Data Protection Laws and Individual Rights

The United Kingdom (UK) has built one of the most detailed and protective systems in the world for managing personal data and technology use. Two key laws guide this system: the Data Protection Act 2018 (DPA 2018) and the UK General Data Protection Regulation (UK GDPR). Together, these laws set out how personal and sensitive data can be collected, stored, used, and shared. They are especially important for Internet of Things (IoT) and Internet of Bodies (IoB) technologies, because these systems collect huge amounts of personal data, often without the user's active involvement. For instance, fitness trackers, smart watches, health implants, and home monitoring devices all gather information automatically.

Section 35(1) of the Data Protection Act[106] clearly states that personal data must only be processed when it is necessary and proportionate. This means that organisations and companies cannot collect more information than is needed for a specific purpose. They also must inform individuals about what kind of data is collected, how it is stored, and why it is being used. This principle of lawfulness, fairness, and transparency ensures that people are not unknowingly monitored or tracked.

The UK GDPR, which replaced the European Union GDPR after Brexit, strengthens these rights even more. **Article 6 of the UK GDPR** [107]outlines the legal bases for processing data. A company or public authority must show that data processing is justified under one of the following: (1) consent of the individual, (2) a legal obligation, (3) performance of a contract, (4) protection of vital interests, (5) public task, or (6) legitimate interests.[108]

For IoB technologies, this is particularly important because they often collect health-related, genetic, or biometric data information that can reveal intimate details about a person's body or mind. **Article 9(1) of the UK GDPR**[109]refers to these as "special categories of personal data" and gives them extra protection. Such data cannot be processed unless the person has given explicit consent, or if it is necessary for public health, medical research, or similar scientific purposes. For example, a company developing a brain-computer interface must first seek clear consent from the user before recording neural data. This approach protects people from the misuse of their biological and mental information.

The UK framework places individuals known as data subjects at the centre of control. They have rights to access their data, to correct inaccurate information, to limit processing, and even to demand deletion of their data under **Article 17 of the UK GDPR** (the "right to be forgotten").[110] These rights empower people to decide what happens to their personal information and ensure companies act responsibly.

---

[106] Data Protection Act 2018

[107] General Data Protection Regulation (UK GDPR). (2018). *Regulation (EU) 2016/679 as retained in UK law by the European Union (Withdrawal) Act 2018.* London: The Stationery Office. Retrieved from https://www.legislation.gov.uk

[108] General Data Protection Regulation (UK GDPR). (2018). Regulation (EU) 2016/679 as retained in UK law by the European Union (Withdrawal) Act 2018. London: The Stationery Office. Retrieved from https://www.legislation.gov.uk

[109] Ibid

[110] Ibid

4.1.2 Enforcement and Accountability Mechanisms

To make sure these privacy laws are followed, the UK has a strong enforcement body known as the **Information Commissioner's Office (ICO)**. The ICO oversees data protection compliance, investigates complaints, and can impose penalties on organisations that break the law. According to **Section 155(2) of the Data Protection Act 2018[111] and Article 83 of the UK GDPR[112]**, the ICO can issue administrative fines of up to **£17.5 million or 4% of a company's global annual turnover**, whichever is higher. These high fines serve as a warning to organisations that fail to protect people's data.

The ICO also plays an educational role. It regularly publishes guidance and codes of practice on how to handle new and emerging technologies like IoT, artificial intelligence (AI), and automated decision-making systems. For example, the ICO's guidance on **"AI and Data Protection" (2020)** explains how companies developing smart devices must integrate privacy safeguards into their design. This idea is known as *"privacy by design and by default"* and is also supported under **Article 25 of the UK GDPR**.[113]

Accountability is a key part of the UK's approach. Organisations that process large amounts of personal data must appoint a **Data Protection Officer (DPO)** under **Article 37 of the UK GDPR**.[114] The DPO ensures that all operations comply with data protection principles and reports directly to senior management. Furthermore, companies must carry out **Data Protection Impact Assessments (DPIAs)** before starting any project that could pose high risks to individuals' privacy, as required under **Article 35**. This ensures that privacy risks are identified and reduced early in the development process, especially for IoT and IoB systems that handle sensitive health or biometric data.

This strong regulatory environment has built public confidence in how personal data is handled. For instance, in 2021 the ICO fined British Airways £20 million after a major data

---

[111] Data Protection Act 2018

[112] General Data Protection Regulation (UK GDPR). (2018). Regulation (EU) 2016/679 as retained in UK law by the European Union (Withdrawal) Act 2018. London: The Stationery Office. Retrieved from https://www.legislation.gov.uk

[113] [113] General Data Protection Regulation (UK GDPR). (2018). Regulation (EU) 2016/679 as retained in UK law by the European Union (Withdrawal) Act 2018. London: The Stationery Office. Retrieved from https://www.legislation.gov.uk

[114] Ibid

breach exposed customer details. The fine reminded companies that failure to secure data properly is a serious offence. By enforcing such penalties, the UK ensures that companies adopt better cybersecurity and privacy practices.

4.1.3 Cybersecurity and Protection Against Digital Threats

While data protection laws focus on how information is used, the UK also has specific laws to protect against **cybercrime** and **technological misuse**. The **Computer Misuse Act 1990 (CMA)** is one of the strongest cybercrime laws in the United Kingdom. It was introduced to protect computer systems and data from unauthorised access, hacking, and digital interference. Section 1 of the Act makes it a criminal offence to access a computer without permission, even if no damage is done. This means that simply breaking into another person's computer system or device without consent is illegal. Section 3 takes this protection further by making it an offence to do any unauthorised act with the intention of impairing the operation of a computer or being reckless as to whether such impairment might occur. According to **Section 3(1)**,[115] a person commits an offence if they perform any unauthorised act on a computer, knowing it is unauthorised, and either intend to impair its function or are reckless about the possibility of doing so. Subsection (2) explains that this includes actions meant to stop access to data, damage computer programs, or reduce the reliability of stored information. The section also clarifies under **Section 3(5)** that an "act" includes a series of actions and that even temporary interference counts as impairment. A person found guilty under this provision may face up to **ten years imprisonment** or a fine, as stated in **Section 3(6)(c)**.

Section 3ZA of the Act[116], titled *Unauthorised Acts Causing, or Creating Risk of, Serious Damage*, deals with more severe offences involving harm to people, the economy, or national security. Under **Section 3ZA(1)**,[117] it is an offence to perform any unauthorised act on a computer knowing that it is unauthorised, where the act either causes or creates a significant risk of serious damage. "Serious damage" in this section refers to harm to human welfare, the environment, the economy, or national security. The law gives practical examples under **Section 3ZA(3)[118]**, stating that damage to human welfare

[115] Computer Misuse Act 1990 Chapter 18
[116] Ibid
[117] Ibid
[118] Ibid

includes loss of life, injury, illness, or disruption of essential services such as money supply, water, energy, transport, communication, or healthcare. This provision is very relevant to IoT and IoB technologies because interference with connected health devices, such as pacemakers or hospital monitoring systems, can cause serious harm or even death. Therefore, the law protects not only computers and networks but also human safety and public welfare. Under **Section 3ZA(6)**, a person convicted of this offence may face up to **fourteen years imprisonment** or a fine. However, if the offence causes or risks causing death, serious injury, or major harm to national security, **Section 3ZA(7)**[119] allows for **life imprisonment**. This strict punishment shows how seriously the UK treats cybercrimes that endanger lives or threaten the country's safety.

In addition to the CMA, the **Cyber Security Breaches Regulations 2018** require certain organisations to report serious cybersecurity incidents to relevant authorities within 72 hours. This ensures quick responses and limits the damage of cyberattacks. The **National Cyber Security Centre (NCSC)**, established under the Government Communications Headquarters (GCHQ), also plays a major role in protecting public and private systems from cyber threats.[120]

The NCSC developed the **Code of Practice for Consumer IoT Security (2018)**, which sets out 13 practical guidelines for device manufacturers. These include using unique passwords for each device, providing regular security updates, protecting stored and transmitted data, and making it easy for users to delete personal data. Manufacturers are also encouraged to clearly state how long devices will receive updates and to avoid hardcoded default passwords, which are a common security weakness.[121]

These rules make IoT devices safer from design to use. For instance, if a smart home camera or wearable health tracker follows the NCSC Code, it becomes much harder for hackers to break in and access private footage or biometric data. This approach, called *security by design*, reduces risks before devices even reach consumers.

4.1.4 Human Rights Protection and Judicial Oversight

[119] Computer Misuse Act 1990 Chapter 18

[120] National Cyber Security Centre (NCSC). (2018). *Code of Practice for Consumer IoT Security: Guidance for Manufacturers.* London: NCSC. Retrieved from https://www.ncsc.gov.ukn

[121] National Cyber Security Centre (NCSC). (2018). *Code of Practice for Consumer IoT Security: Guidance for Manufacturers.* London: NCSC. Retrieved from https://www.ncsc.gov.uk

Beyond data and cybersecurity laws, the UK protects personal privacy through **human rights legislation**. The **Human Rights Act,**[122] incorporates the **European Convention on Human Rights (ECHR)** into domestic law. **Article 8 of the ECHR** guarantees everyone the right to respect for their *private and family life, home, and correspondence*. This right covers all aspects of privacy, including digital and technological privacy.

UK courts have interpreted Article 8 broadly to include protection against intrusive surveillance, facial recognition, and the collection of personal data without consent. A key case that demonstrates this is **R (Bridges) v Chief Constable of South Wales Police [2020] EWCA Civ 1058**.[123] In this case, the police used automatic facial recognition (AFR) technology in public places without a clear legal framework or sufficient safeguards. The Court of Appeal ruled that this use violated **Article 8 of the ECHR**[124], as it interfered with privacy rights without adequate justification or oversight. The Court also held that the police had failed to conduct a proper data protection impact assessment under the DPA 2018 and UK GDPR.

This ruling was a landmark for technology regulation. It showed that even when law enforcement or public authorities use advanced technologies, they must still respect human rights and data protection principles. The decision also encouraged the development of clearer policies and greater transparency in the use of AI and biometric systems across the UK.

The Human Rights Act also connects to IoB technologies, which have the potential to access and record data directly from the human body or brain. If such technologies are misused, they could infringe on human dignity and bodily autonomy. Through Article 8, courts can ensure that such innovations do not undermine these fundamental values.

4.2 LESSONS FOR ZAMBIA FROM THE UK FRAMEWORK

Zambia can learn several lessons from the UK's approach. First, it should adopt clear and specific rules for handling biometric and neurological data as "special categories of data," requiring explicit consent and strict safeguards. Second, it can strengthen the powers of the Data Protection Commissioner to enforce compliance and impose heavy fines for

[122] Human Rights Act 199

[123] R (Bridges) v Chief Constable of South Wales Police [2020] EWCA Civ 1058 (Court of Appeal, United Kingdom).

[124] European Convention on Human Rights. (1950). *Convention for the Protection of Human Rights and Fundamental Freedoms.* Rome: Council of Europe. Retrieved from https://www.echr.coe.int

violations. Third, it can promote a “privacy by design” approach, ensuring that IoT and IoB devices include security and privacy protections from the development stage. Finally, judicial oversight, as demonstrated in the Bridges case, shows the importance of an active judiciary in interpreting constitutional rights in the digital age.

4.3 THE KENYA LEGAL FRAMEWORK FOR IOT AND IOB TECHNOLOGIES

Kenya has made significant progress in protecting personal data and strengthening its digital laws. The main law that governs how personal data is handled is the **Data Protection Act,** This Act was designed to be consistent with international best practices, particularly the **European Union’s General Data Protection Regulation (GDPR)**. It ensures that personal information is collected and used responsibly, with respect for privacy and human dignity.

Under **Section 2 of the Act,** *personal data* is defined as any information relating to an identified or identifiable person.[125] This includes a person’s name, identification number, location, and importantly, **biometric and health data**. This wide definition makes the Act well suited to modern technologies such as the **Internet of Things (IoT)** and the **Internet of Bodies (IoB)**, which collect large amounts of personal and biological data through connected devices, sensors, and implants.

The **Data Protection Act,[126]** places a strong duty on organisations that collect or process data. **Section 25[127]** provides that data controllers and data processors must ensure that personal data is processed *lawfully, fairly, and transparently*. It must also be collected for a *specific and legitimate purpose*, and not used in a way that is incompatible with that purpose. For IoT and IoB technologies, this means that companies and health providers cannot collect more data than is necessary or use it for hidden purposes. For instance, if a wearable fitness device collects data for health tracking, that data cannot later be sold to advertisers without consent.

The same section also requires that organisations keep personal data secure and protect it from *unauthorised access, loss, or misuse*. This duty is critical because IoT devices constantly communicate across networks, and without strong safeguards, hackers could

[125] Data Protection Act, No. 24 of 2019
[126] Data Protection Act, No. 24 of 2019
[127] Ibid

access sensitive data. The law therefore promotes “data security by design,” encouraging developers to build privacy protections directly into their technologies.

Furthermore, **Section 3[128]1** requires organisations to carry out a **Data Protection Impact Assessment (DPIA)** before engaging in any processing activity that could pose a high risk to individuals’ rights and freedoms. This applies especially to IoB technologies, such as brain-computer interfaces or biometric implants, where the misuse of data could seriously harm human autonomy or expose private health information. A DPIA helps identify these risks early and ensure that the right safeguards are in place.

4.3.1 Enforcement, Oversight, and Remedies

To ensure that data protection rules are followed, the Data Protection Act, 2019 established a strong oversight body known as the Office of the Data Protection Commissioner (ODPC). The ODPC was created under **Section 5 of the Act** as an independent institution responsible for enforcing data protection standards, investigating complaints, and promoting awareness about privacy rights. The Commissioner also advises government agencies and private organisations on how to comply with the law when using technology that collects personal data.

The ODPC has wide powers to take action against anyone who violates the Act. Under **Section 63**[129], the Commissioner can issue administrative fines or compliance orders to any data controller or processor that fails to follow the rules. This means that companies must take their data protection duties seriously or face legal and financial consequences. For example, if an IoT company fails to protect user data and a data breach occurs, the ODPC can impose a fine or order the company to fix its security systems immediately.

Individuals, known as data subjects, also have strong rights under Kenyan law. Section 26 gives them several key powers: the right to be informed when their data is collected, the right to access their personal data, the right to object to its processing, and the right to request correction or deletion of inaccurate information. These rights ensure that people remain in control of their personal information even when it is held by large organisations.

[128] Data Protection Act, No. 24 of 2019

[129] Data Protection Act, No. 24 of 2019

The ODPC also plays a public role by publishing guidelines and educating people about their digital rights. In recent years, the Commissioner has issued advisories on the use of CCTV cameras, digital health platforms, and mobile applications that process sensitive data. Such efforts are helping to build a culture of privacy and accountability across Kenya's fast-growing digital economy.

4.3.2 Cybersecurity and Digital Safety

Kenya has strengthened its digital safety framework through the Computer Misuse and Cybercrimes Act, 2018. The Act protects digital systems, including IoT and IoB devices, by criminalising unauthorised access under **Section 14**[130]and interference with data or systems under **Section 15.**[131] It also addresses online offences such as cyberstalking, identity theft, and false information through **Sections 27 to 33**[132]. To support national security, Section 4 creates the National Computer and Cybercrimes Coordination Committee, which promotes cooperation between agencies and private institutions to detect and prevent cyber threats.

Kenya's constitutional protection of privacy forms the backbone of its digital laws. **Article 31 of the Constitution**[133] guarantees every person the right to privacy and prohibits unnecessary intrusion into personal information or property. Kenyan courts have applied this provision to digital spaces, as seen in CORD v Attorney General [2015] eKLR, where the High Court ruled that surveillance measures must respect constitutional safeguards. This shows that the right to privacy applies even as technology evolves and devices collect sensitive personal and biological data.

Beyond privacy, the Constitution guides how Kenya regulates digital innovation. **Article 10**[134] promotes national values such as human rights, good governance, and integrity, ensuring that laws like the Data Protection Act and the Cybercrimes Act are applied in a manner that prioritises people's wellbeing. This constitutional foundation helps ensure

[130] Computer Misuse and Cybercrimes Act, No. 5 of 2018
[131] Ibid
[132] Ibid
[133] Constitution of Kenya, 2010.
[134] Constitution of Kenya, 2010.

that technological growth remains responsible, transparent, and respectful of individual freedoms.

4.4 LESSONS FOR ZAMBIA FROM THE KENYA FRAMEWORK

Zambia can learn valuable lessons from Kenya's legal reforms. First, it should strengthen its definition of personal data to include biometric, genetic, and neurological information. Second, Zambia could adopt mandatory Data Protection Impact Assessments for IoT and IoB systems to ensure risks are identified before deployment. Third, Zambia can empower the Data Protection Commissioner with stronger enforcement powers, similar to Kenya's ODPC, to ensure real accountability. Fourth, incorporating clear constitutional recognition of digital privacy, as seen in Kenya's Article 31, would make Zambia's protections more future-proof.

4.5 CONCLUSION

both the United Kingdom and Kenya have shown that clear laws, strong enforcement, and respect for human rights are essential in managing IoT and IoB technologies. The UK's approach demonstrates the importance of detailed data protection rules, strict cybersecurity standards, and effective enforcement through institutions such as the Information Commissioner's Office. Kenya's system, guided by its Constitution and modern data protection laws, shows how developing countries can build digital trust and protect citizens in a connected world. From these examples, Zambia can learn to strengthen its data protection laws, adopt strict penalties for cyber offences, promote privacy and security by design, and empower regulators to oversee technology use effectively. These lessons will help Zambia create a balanced legal framework that supports innovation while protecting human dignity and personal privacy in the digital era.

CHAPTER FIVE

CONCLUSIONS AND RECOMMENDATIONS

5.0 INTRODUCTION

This chapter presents the conclusions and recommendations of the study on the adequacy and appropriateness of Zambia's legal framework governing the Internet of Things (IoT) and the Internet of Beings (IoB). It summarizes the key findings from the previous chapters, highlighting the major issues identified and the lessons Zambia can draw from international, regional, and comparative experiences. The chapter begins by outlining the findings from Chapters One to Four, which covered the background of the study, the international and regional legal frameworks, Zambia's domestic legal framework, and comparative insights from the United Kingdom and Kenya. It then provides practical recommendations aimed at strengthening Zambia's legal and institutional mechanisms to ensure that IoT and IoB technologies are managed in a way that protects human rights, promotes accountability, and supports responsible technological innovation.

5.1 FINDINGS AND CONCLUSIONS

5.1.1 CHAPTER ONE

Chapter one gave a general overview of the topic and set the foundation on the adequacy and appropriateness of the legal framework governing internet of things and internet of beings in Zambia. It gave a brief background to the study; further, it looked at the statement of the problem, objectives of the study, research questions and significance. Then, a literature review was given stating how the study differs from other authors and finally the methodology of the study.

5.1.2 CHAPTER TWO

This chapter was based on the international legal framework that governs the use of Internet of Things (IoT) and Internet of Beings (IoB) technologies. It examined how international and regional instruments such as the Universal Declaration of Human Rights (UDHR), the International Covenant on Civil and Political Rights (ICCPR), the General Data Protection Regulation (GDPR), the Budapest Convention on Cybercrime, and the Malabo Convention provide protection for privacy, data, and human dignity. The chapter

found that while these instruments were not originally made for digital technologies, their principles still apply and help guide how states regulate IoT and IoB systems that collect, store, and use personal information.

The findings show that **Article 12 of the UDHR** and **Article 17 of the ICCPR** protect privacy and human dignity, forming the moral and legal base for regulating intrusive technologies. The **GDPR**, especially **Article 6**, sets strong rules for lawful data processing and emphasizes privacy by design, giving individuals rights such as consent, access, correction, and deletion of their data. The **Budapest Convention**, through **Articles 2 to 6**, deals with cybercrimes such as illegal access, interception, and data interference, which are common threats to IoT and IoB devices. The **Malabo Convention**, particularly **Articles 8, 9, 10, 13, and 25**, adds African regional standards that stress lawful processing, informed consent, state responsibility, and criminal liability for data misuse.

The chapter found that these international and regional laws together create a strong foundation for protecting people in the digital age. They ensure that as IoT and IoB technologies grow, privacy, dignity, and safety are not ignored. However, more countries, especially in Africa, need to ratify and enforce these frameworks so that people's data and bodily integrity are fully protected under clear and uniform rules.

5.1.3 CHAPTER THREE

This chapter was based on Zambia's legal and regulatory framework governing the Internet of Things (IoT), the Internet of Beings (IoB), and the protection of human rights. The findings show that Zambia's Constitution and related laws provide a strong foundation for protecting rights such as privacy, dignity, and liberty, but they were written before the rise of advanced digital and biological technologies. Article 11 of the Constitution guarantees fundamental rights and freedoms, while Article 17 protects privacy and Article 15 upholds dignity and protection from inhuman treatment. However, these provisions mainly deal with physical intrusions and do not clearly cover digital or biological invasions caused by IoT and IoB devices. The chapter found that new forms of "mental privacy" and "biological autonomy" are not expressly recognized under the current constitutional language, creating a legal gap.

The Data Protection Act aims to regulate the collection and use of personal data, but Section 3 lacks clarity on what "personal use" means. Section 12(1) sets key principles

of data processing, yet it does not deal with complex IoB data such as brain activity or emotional patterns. Section 13, which allows data processing based on “legitimate interest,” can easily be abused, while Sections 58 to 65 give individuals data rights that are hard to exercise because most IoT and IoB devices collect data automatically and secretly.

The Cyber Security Act No. 3 of 2025 and the Cyber Crimes Act No. 4 of 2025 strengthen the fight against unauthorized interception and cyber offences under Sections 22, 29, and 3(1), but they also have gaps. They do not specifically protect biological or neurological data produced by IoB devices, leaving users exposed to risks such as thought surveillance and bodily interference.

Zambia has made real progress through its constitutional and statutory laws, but these laws are still limited in addressing the challenges of IoT and IoB. The existing framework protects traditional rights but not the new digital and biological dimensions of privacy, dignity, and freedom of thought. Therefore, legal reforms are needed to include clearer protections for mental and bodily integrity to ensure that technological innovation does not weaken fundamental human rights.

5.1.4 CHAPTER FOUR

This chapter was based on the lessons that Zambia can learn from the United Kingdom and Kenya in managing and protecting the use of Internet of Things (IoT) and Internet of Bodies (IoB) technologies. The findings show that both countries have developed strong legal systems that balance innovation with the protection of privacy, data, and human dignity. The United Kingdom relies on the **Data Protection Act 2018**, the **UK GDPR**, and the **Computer Misuse Act 1990**, which provide clear rules for data processing and strong safeguards for individuals. Under **Section 35(1)** of the Data Protection Act, personal data must only be processed when necessary, while **Article 6** and **Article 9(1)** of the UK GDPR protect sensitive and biometric data, requiring explicit consent before use. The **Information Commissioner’s Office (ICO)** enforces these laws, and **Article 8 of the Human Rights Act** ensures that privacy is treated as a fundamental human right, as confirmed in *R (Bridges) v Chief Constable of South Wales Police [2020]*.

In Kenya, the **Data Protection Act 2019** and the **Computer Misuse and Cybercrimes Act 2018** form the foundation of its digital legal system. **Section 25** of the Data Protection

Act requires fair and lawful data processing, while **Section 31** of the Constitution guarantees every person the right to privacy. The **Office of the Data Protection Commissioner (ODPC)**, established under **Section 5**, enforces compliance, and **Section 63** empowers it to fine violators. The Kenyan High Court in *CORD v Attorney General [2015]* confirmed that surveillance must not breach privacy rights, ensuring digital technologies respect human dignity.

Both the United Kingdom and Kenya show that strong privacy laws, active enforcement, and respect for human rights can guide safe use of IoT and IoB technologies. Zambia can learn from these systems by clearly defining sensitive data, introducing strict penalties for misuse, strengthening its data protection authority, and ensuring its laws protect both digital and biological privacy in the modern era.

5.2 RECOMMENDATION

This research has revealed that Zambia's legal framework for managing the Internet of Things (IoT) and the Internet of Bodies (IoB) lacks strong protection mechanisms for data privacy, enforcement, and technological oversight compared to the systems in the United Kingdom and Kenya. The author therefore recommends the following:

1. Introduce Specific Protection for Biological and Neurological Data

Zambia should amend the Data Protection Act to include explicit provisions that recognize and protect sensitive IoB data such as brain activity, emotional patterns, and biometric information. This could be done by expanding the definition of "sensitive personal data" under Section 2 and adding new rules in Section 12(1) to address the handling, storage, and transfer of such data. This would safeguard citizens' mental privacy, dignity, and bodily autonomy from misuse by both private entities and the State.

2. Clarify and Strengthen the Scope of "Personal Use" and "Legitimate Interest"

The Data Protection Act should clearly define what "personal use" under Section 3 means to avoid misuse by individuals or companies processing data through personal devices such as smart home systems. Likewise, Section 13(b)(v), which allows data processing based on "legitimate interest," should be tightened by introducing clear criteria and requiring prior authorization from the Data Protection Commissioner for sensitive IoB-related processing. These reforms would reduce legal uncertainty and prevent abuse of personal and biological data.

3. Enhance Oversight and Enforcement Mechanisms for IoT and IoB Regulation

The government should strengthen the enforcement powers of the Data Protection Commissioner and the Human Rights Commission to monitor and investigate IoT and IoB technologies. This could include creating a specialized "Digital Rights and Emerging Technologies Unit" within these institutions to oversee compliance with data and human rights standards. Additionally, Zambia should establish cross-border cooperation frameworks to hold foreign companies accountable when they process Zambian citizens' data abroad. Such measures would ensure that technological growth is balanced with effective human rights protection in the digital era.

4. Strengthen Legal Protection for Digital and Biological Data

Zambia should amend its Data Protection Act to clearly define and protect sensitive data, including biometric and biological information generated through IoT and IoB devices. This can be done by expanding the definition of "sensitive personal data" and requiring explicit consent before processing such information, similar to Article 9(1) of the UK GDPR. This would ensure individuals' privacy, bodily integrity, and human dignity are protected in the digital environment.

5. Establish an Independent Data Protection Authority

Zambia should create or strengthen an independent data protection body, similar to the Information Commissioner's Office (ICO) in the United Kingdom and the Office of the Data Protection Commissioner (ODPC) in Kenya. This authority should have clear powers to monitor, investigate, and impose penalties for misuse of personal or biological data. Empowering such a body would ensure accountability, promote compliance, and enhance citizens' trust in emerging technologies.

6. Introduce Clear Penalties and Compliance Frameworks for IoT and IoB Violations

The government should develop specific penalties for breaches involving IoT and IoB systems, modeled on the enforcement provisions in Section 63 of Kenya's Data Protection Act. These penalties should cover unauthorized data collection, storage, or transfer of personal and biological information. Additionally, mandatory compliance frameworks and periodic audits should be introduced to ensure that both local and foreign technology operators uphold Zambia's data protection and human rights standards.

BIBLIOGRAPHY

Books

Nicol, C. (2003). ICT Policy: A Beginner's Handbook. Association for Progressive Communications.

Journal Articles

Boshe, Patricia. (2016). Data Privacy Law Reforms in Tanzania. In Makulilo, A. B. (Ed.), African Data Privacy Laws. Springer.

Bowen, G. A. (2009). Document analysis as a qualitative research method. Qualitative Research Journal, 9(2), 27–40. https://studylib.net/doc/26180343/bowen-2009-document-analysis-as-a-qualitative-method

Jones, A., & Patel, R. (2019). Protecting Privacy in the Digital Age: Legal Challenges and Solutions. International Journal of Law and Technology, 8(3), 211–230.

Kugler, K. (2022). The Impact of Data Localisation Laws on Trade in Africa. Mandela Institute.

Makulilo, A. B. (2016). African Data Privacy. Springer International Publishing.

Michael Phillips. (2013). A New Legal Theory for the Age of Mass Surveillance.

Mwansa, A. (2015, September 11). ICT policy will attract investors. Zambia Daily Mail.

Polat, R. K. (2012). Digital exclusion in Turkey: A policy perspective. Government Information Quarterly, 29(4), 589–596.

Smith, J. (2020). The Intersection of Privacy Rights and Data Protection: A Comparative Analysis. Journal of Comparative Law, 15(2), 123–145.

Soka, Zimba, & Chembe, Christopher. (2022). Model for Water Quality Monitoring Based on Internet of Things. Volume 6(1), 44–51.

Souter, D. (2009). The APC ICT Policy Handbook. Association for Progressive Communications.

Zimba, S., & Chembe, C. (2022). Model for Water Quality Monitoring Based on Internet of Things. Zambia ICT Journal, 6(1), 44–51.

International Instrument

African Union. (2014). *African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention).* Adopted in Malabo, Equatorial Guinea, 27 June 2014. Retrieved from https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection

Council of Europe, *Convention on Cybercrime* (Budapest, 23 November 2001) ETS 185, https://rm.coe.int/1680081561 accessed 18 September 2025.

European Commission, 'Data Protection in the EU' (European Commission, 2023) https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_en accessed 18 September 2025.

European Convention on Human Rights. (1950). Convention for the Protection of Human Rights and Fundamental Freedoms. Rome: Council of Europe. Retrieved from https://www.echr.coe.int

European Data Protection Board, 'Guidelines on Data Protection by Design and by Default' (EDPB, 2020) https://edpb.europa.eu/ accessed 18 September 2025.

Media Defence. (2021). The African Union's Malabo Convention and data protection in Africa. Retrieved from https://www.mediadefence.org

United Nations. (1948). *Universal Declaration of Human Rights (UDHR)*. Adopted by the UN General Assembly Resolution 217 A (III). Retrieved from https://nations-united.org/Universal_Declaration_Of_Human_Rights/Articles_Human_Rights/Articles_12_Human_Rights_Universal_Declaration_Nations_United_Twelve.htm

United Nations. (1966). *International Covenant on Civil and Political Rights (ICCPR)*. Adopted by UN General Assembly Resolution 2200A (XXI). Retrieved from https://legal.un.org/avl///ha/iccpr/iccpr.html

Dissertations

Faith Mwafulirwa (2023) The Internet of Things: Is The Zambian Law Adequate?. the University of Lusaka

Hanyama, N. (2018). Policies and Legislation for Internet Access and Usage in Zambia. University of Zambia.

Report

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1.

National Cyber Security Centre (NCSC). (2018). *Code of Practice for Consumer IoT Security: Guidance for Manufacturers.* London: NCSC. Retrieved from https://www.ncsc.gov.ukn

Internet Sources

GDPR.eu, 'What is GDPR, the EU's new data protection law?' (GDPR.eu, 2023) https://gdpr.eu/what-is-gdpr/ accessed 18 September 2025.

Information Commissioner's Office (ICO), 'Guide to the UK General Data Protection Regulation (UK GDPR)' (ICO, 2023) https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/

EDRi-gram. (2015). 300 issues of EDRi-gram. Retrieved from https://www.wired.com/beyond-the-beyond/2015/05/300-issues-edri-gram

ZAMBIA - Enforcement of the Data Protection Act No. 3 of 2021 Begins in March 2025 https://www.nadpa-rapdp.org/en/node/220 (Accessed 19/04/2025)

https://www.emnify.com/blog/iot-security#:~:text=The%202016%20Mirai%20botnet,but%20also%20because%20the (Accessed 19/04/2025)

https://www.statista.com/outlook/tmo/internet-of-things/zambia (Accessed 19/04/2025)

UNIVERSITY OF LUSAKA

SCHOOL OF LAW

L400B – DIRECTED RESEARCH (OBLIGATORY ESSAY)

RESEARCH CLEARANCE FORM

NAME: ABIGAIL M. N. MWAPULE STUDENT NUMBER: 4482211429

SUPERVISOR: MRS. KAPUTO TOPIC: THE ADEQUACY AND APPROPRIATENESS OF THE LEGAL FRAMEWORK GOVERNING INTERNET OF THINGS AND INTERNET OF BEINGS IN ZAMBIA

Stage	Comments	Supervisor's Signature & Date	Student's Signature & Date
Research Proposal	few minor changes.	12/08/25	12/08/25
Chapter 1 – Introduction	Refine the objectives	6/10/25	6/10/25
Chapter 2 –	minor changes.	6/10/25	6/10/25
Chapter 3 –	approved	6/10/25	6/10/25
Chapter 4 –	Approved	5/11/25	5/11/25
Chapter 5 – Conclusions & Recommendations	Approved	5/11/25	5/11/25
Table of Contents, Bibliography and Appendices	Okay to proceed	5/11/25	5/11/25
First Draft	approved	12/11/25	12/11/25

Second Draft			
Final Draft	okay to submit	12/11/25	12/11/25

*Please return this form to the LLB Research Coordinator at the end of the research.

Report #29955949

SCHOOL OF LAW THE ADEQUACY AND APPROPRIATENESS OF THE LEGAL FRAMEWORK GOVERNING INTERNET OF THINGS AND INTERNET OF BEINGS IN ZAMBIA BY ABIGAIL M. 6 7 N MWAPULE LLB22114289 An obligatory essay submitted to the University of Lusaka in partial fulfillment of the requirement for the award of the Bachelor of Laws (LLB) Degree 2025 i DECLARATION I ABIGAIL M. 1 2 3 4 5 6 7 N MWAPULE do declare that this dissertation titled 1 2 3 4 5 6 7 "THE ADEQUACY AND APPROPRIATENESS OF THE LEGAL FRAMEWORK GOVERNING INTERNET OF THINGS AND INTERNET OF BEINGS IN ZAMBIA" 1 2 3 4 5 6 7 which is hereby submitted to the School of Law at the University of Lusaka as part of the requirements for the award of the Bachelor of Laws (LLB) degree is my original work and has not previously been submitted for the award of a degree at this or any other tertiary institution. 1 2 3 4 6 7 The sources that have been used or quoted have been indicated and duly acknowledged as complete reference Signature……... 1 2 3 4 5 6 7 Date: 14/11/2025 ii SUPERVISOR'S RECOMMENDATION I Do hereby recommend that this dissertation titled 1 2 3 4 5 6 7 "THE ADEQUACY AND APPROPRIATENESS OF THE LEGAL FRAMEWORK GOVERNING INTERNET OF THINGS AND INTERNET OF BEINGS IN ZAMBIA" 1 2 3 4 5 6 7 done under my supervision be admitted by the university I have